## Amendments to the Specification

**Page 6 lines 3-16:**

With respect to other IPSec protocols such as IKE (see, e.g., D. Maughan, M. Schertler, M. Schneider and J. Turner, "Internet Security Association and Key Management Protocol [ISAKMP]," IETF, RFC 2408, Nov. 1998; and D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," IETF, RFC 2409, Nov. 1998) and the ESP tunnel protocol, Linux's NAT implementation, called IP Masquerade, includes a feature called VPN Masquerade ~~(see, e.g., "Linux VPN Masquerade",~~ ~~http://www.impsec.org/linux/masquerade/ip_masq_vpn.html)~~, which provides NAT interoperation with the IKE and ESP tunnel protocols. IKE is used for negotiation of cryptographic protocols, algorithms, and keys and the ESP tunnel mode is described above. NAT support for these protocols is possible because they do not authenticate or encrypt any information that depends on the IP header of the packet itself (IKE) or encapsulating packet (ESP tunnel mode), unlike the AH and ESP transport modes.

**Page 20, lines 8-11:**

In accordance with the present invention, the client software ~~325~~ 320 running on each client 301 that implements, in this embodiment, the IPSec protocol, prevents at least some of these race conditions and/or recovers from crashes or collisions.

**Page 25, lines 8-24:**

After a tunnel epoch is established, at step 602, if, at step 621, the client fails to receive anything from the tunnel for a predetermined period of time, MAXIDLE, then it will attempt to keep the item established in the NAT by "pinging" the server. At step 615, a counter, NTRIES2, is set at zero. At step 616, the client "pings" the server. If, at step 617, the client receives a reply to its "ping" from the server before predetermined timeout period, PINGTIME2, which may be the same as the timeout period PINGTIME noted above, then the epoch remains active and the flow returns to step 602. If, however, the client does not

receive a reply from the server to this "ping", then, at step 618, NTRIES2 is incremented by one and, at step 619, NTRIES2 is compared with PINGTRIES2, which may be the same value as PINGTRIES ~~note~~ noted above. If NTRIES2 is less than or equal to PINGTRIES2, then the client sends another "ping" to the server, at step 616. If NTRIES2 is greater than PINGTRIES2, then the flow returns to step 603, where NEPOCH is reset to zero, and where thereafter, the client starts a negotiation for a new epoch. If the time limit MAXIDLE is set sufficiently low, then by successfully "pinging" the server, the item remains active and starting a new epoch due to tunnel inactivity is not likely to occur.